Effects of Quantization and Dithering in Privacy Analysis for a Networked Control System

Kawano, Yu; Cao, Ming

Published in:
2021 60th IEEE Conference on Decision and Control (CDC)

DOI:
10.1109/CDC45484.2021.9683078

Publication date:
2022

2021 60th IEEE Conference on Decision and Control (CDC)
December 13-15, 2021. Austin, Texas

Effects of Quantization and Dithering in Privacy Analysis for a Networked Control System*

Yu Kawano[1] and Ming Cao[2]

2021 60th IEEE Conference on Decision and Control (CDC) | 978-1-6654-3659-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CDC45484.2021.9683078

***Abstract*— In digital communication networks, typically information is sent after quantization. When such quantized information is used by controllers, it is known that quantization is very likely to degenerate control performance. In contrast, we show in this paper the interesting finding that quantization may improve privacy performance of the networked subsystems under control. Namely, there is a trade-off between control and privacy performances determined by the quantization step. In this paper, we look at a *dither* (also called random dithered quantizer) as a possible tool to improve both control and privacy performances for networked systems. We review some known improved control performances such as in sampling, and then further discuss the effects of a dither in privacy analysis.**

I. Introduction

A key feature of IoT technologies is to share data through networks, which may create the risk of one user's private information being inferred by other users. To address such threats, privacy protection has been studied in various fields, see e.g. [1]–[4] for references in system and control. Note that these papers mainly focus on statistical disclosure control methods. In IoT technologies, information is typically sent after quantization. Utilities of quantizers are illustrated by security of encrypted control systems [5], [6], where in this paper, by security we mean data protection against adversaries, and in comparison by privacy we mean to prevent one user's data being inferred by other users from shared data. In contrast to security, quantization has not been taken into account in privacy analysis except for [7], [8]; the first paper studies noise design to maximize a privacy level under a prescribed data distortion, and the latter for a static mechanism.

The objective of this paper is to analyze the connection between quantization and privacy. The specific private information considered here is the initial state of a system as formulated in [3], [9]. First, we study how quantization makes estimating the initial state difficult. Because of quantization, the set where the initial state belongs can be described by a family of linear equations. The volume of this set can be viewed as the privacy level, which depends on the quantization step and decreases as time evolves. For Schur stable systems, we show that the number of these linear equations is finite. This means that even if a system is observable, its initial state is not uniquely determined. However, as a negative result, for some unstable system, the initial state can be estimated in arbitrary accuracy.

Although quantization can improve privacy performance, it degenerates control performance. This performance degeneration can be attenuated by adding noise before quantization; such a technique is called *dithering* [10], [11]. Dithering is different from the method in [7] that adds noise after (not before) quantization. In the control context, better control performance is observed for a feedback interconnected system with dithered communication signals [12], [13]. This improvement is due to the feedback loop between dithered signals and state variables.

In this paper, we propose the use of dithering to improve privacy performance. First, we confirm that estimating the initial state becomes more difficult using dithering than quantization. Note that if one considers state estimation, instead of estimating the systems' initial states, the error caused by dithering can be viewed as measurement noise, and thus one may design the Kalman filter. However, this measurement noise is not Gaussian nor does not satisfy the Lindeberg condition [14]. In other words, it is not guaranteed that the Kalman filter works for this state-estimation problem. On the other hand, one may expect that dithering can improve observer performance as for control performance; however, this is not always the case. Because dithered signals do not depend on the observer states, in contrast to the feedback in the control loop, dithering may not improve observer performances. So to quantify observer performances, in this paper, we design the standard Luenberger observer and compute an upper bound on the state estimation error. Our results can be used to evaluate how difficult it is to estimate the state under dithering.

The remainder of this paper is organized as follows. In Section II, we consider quantization and show that for a Schur stable system, a finite set of linear inequalities describes the set where the initial state belongs. In Section III, we consider dithering. First, we show that estimating the initial state becomes more difficult. Next, we compute an upper bound on the state estimation error of an observer. Finally, Section V concludes this paper.

Notation: The sets of real numbers and non-negative integers are denoted by $\mathbb{R}$ and $\mathbb{Z}_+$, respectively. The vector whose all elements are 1 is denoted by $\mathbb{1}$. For two vectors a and b with the same size, $a \preceq b$ ($a \prec b$) stands for the element-wise inequality, namely $a_i \leq b_i$ ($a_i < b_i$) for all elements.

[1]Yu Kawano is with the Graduate School of Advanced Science and Engineering, Hiroshima University, Higashi-Hiroshima, Japan ykawano@hiroshima-u.ac.jp

[2]M. Cao is with the Faculty of Science and Engineering, University of Groningen, Groningen, The Netherlands m.cao@rug.nl

*This work was supported in part by JSPS KAKENHI Grant Number JP21H04875, the European Research Council (ERC-CoG-771687) and the Netherlands Organization for Scientific Research (NWO-vidi-14134)

II. Problem Formulation

Consider the following two subsystems:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t),\ x(0) = x_0, \\ y(t) = Cx(t), \end{cases} \tag{1}$$

$$\begin{cases} \xi(t+1) = F\xi(t) + G\nu(t),\ \xi(0) = \xi_0, \\ \eta(t) = H\xi(t), \end{cases} \tag{2}$$

where $x \in \mathbb{R}^{n_1}$, $\xi \in \mathbb{R}^{n_2}$, $u, \eta \in \mathbb{R}^m$, and $y, \nu \in \mathbb{R}^p$. The matrix dimensions are compatible. These two subsystems are connected via communication networks by which typically quantized information are sent. Specifically, they are interconnected through the quantized couplings:

$$\begin{aligned} u &= \mathcal{Q}(\eta), \\ \nu &= \mathcal{Q}(y), \end{aligned} \tag{3}$$

where the quantizer $\mathcal{Q}$ is defined by

$$\mathcal{Q}(z + nd) = nd \text{ for } z \in \left(-\frac{d}{2}, \frac{d}{2}\right],\ n \in \mathbb{Z}, d > 0. \tag{4}$$

In this paper, we focus on the privacy analysis of each subsystem against the other. In particular, we consider the following scenario.

Scenario 2.1: Consider the two subsystems (1) and (2) interconnected via (3), where each subsystem and the interconnected system with $u = \eta$ and $\nu = y$ are Schur stable. The subsystem (1) aims to protect the information of its initial state x_0 against the subsystem (2) that can access $u(t)$ and $\nu(t) = \mathcal{Q}(y(t))$ at each time instant $t \in \mathbb{Z}_+$ and the triplet (A, B, C). ◁

If the subsystem (1) is observable, and there is no quantization in communication networks, then it is impossible to protect the initial state x_0 against (2). To improve privacy performance, random noise is added to data before sending it [2]–[4]. In fact, quantization can be interpreted as deterministic noise. Throughout this note, we investigate the effect of quantization for privacy protection.

III. Initial State Privacy under Quantization

A. Autonomous Systems

To exclusively evaluate the effect of quantization for protecting the initial state from being identified, first we consider the following autonomous system.

$$\begin{cases} x(t+1) = Ax(t),\ x(0) = x_0, \\ \nu(t) = \mathcal{Q}(Cx(t)), \end{cases} \tag{5}$$

where $x \in \mathbb{R}^{n_1}$ and $\nu \in \mathbb{R}^p$. For analysis purposes, we define the observability matrix and vector consisting of the output sequence as follows:

$$\mathcal{O}_T = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^T \end{bmatrix},\ \nu_T = \begin{bmatrix} \nu(0) \\ \nu(1) \\ \vdots \\ \nu(T) \end{bmatrix}.$$

From the definition (4) of the quantizer $\mathcal{Q}$, if ν_T is observed, the initial state x_0 of the system (5) belongs to the following set:

$$V_T(\nu_T) := \left\{ x_0 \in \mathbb{R}^{n_1} : -\frac{d}{2}\mathbb{1} \prec \mathcal{O}_T x_0 - \nu_T \preceq \frac{d}{2}\mathbb{1} \right\}. \tag{6}$$

The volume of $V_T(\nu_T)$ can be interpreted as a privacy level of the initial state x_0. Since the larger $d > 0$ is, the larger the volume is, quantization increases the privacy level. As T increases, the volume, i.e., the privacy level decreases. It is possible to show that for Schur stable systems, the privacy level does not decrease after sufficient time.

Theorem 3.1: Suppose that the system (5) is Schur stable. For any $x_0 \in \mathbb{R}^{n_1}$ and $\nu : \mathbb{Z}_+ \to \mathbb{R}^p$, there exists $T = T(x_0) \in \mathbb{Z}_+$ such that $V_T(\nu_T) = V_{T+i}(\nu_{T+i})$, $i \in \mathbb{Z}_+$. Moreover, $V_T(\nu_T)$ contains an open subset of $\mathbb{R}^n$.

Proof: First, consider the following set:

$$V_0(0) = \left\{ x_0 \in \mathbb{R}^{n_1} : -\frac{d}{2}\mathbb{1} \prec Cx_0 \preceq \frac{d}{2}\mathbb{1} \right\}, \tag{7}$$

which contains an open subset $U \subset \mathbb{R}^{n_1}$.

Since the system is Schur stable, it admits a Lyapunov function $V(x) = x^\top P x$, where P is symmetric and positive-definite. For this Lyapunov function, there exists $r > 0$ such that

$$\Omega_r := \{x \in \mathbb{R}^{n_1} : x^\top P x \le r\} \subset U \subset V_0(0).$$

This Ω_r is positively invariant. Therefore, from (7), we have

$$-\frac{d}{2}\mathbb{1} \prec Cx(T) \preceq \frac{d}{2}\mathbb{1},\ \forall T \in \mathbb{Z}_+, \forall x_0 \in \Omega_r.$$

In other words, $\Omega_r \subset V_T(0)$ for all $T \in \mathbb{Z}_+$.

Now, we consider an arbitrary initial state. Since the system is Schur stable, for any $x_0 \in \mathbb{R}^{n_1}$ there exists $s = s(x_0) \in \mathbb{Z}_+$ such that $x(s) \in \Omega_r$. Therefore, the statement holds for $T = s$.

Finally, we show that $V_T(\nu_T)$ contains an open subset. From its definition, $V_T(\nu_T)$ is the intersection of a finite number of

$$\hat{V}_t(\nu(t)) := \left\{ x_0 \in \mathbb{R}^{n_1} : -\frac{d}{2}\mathbb{1} \prec CA^t x_0 - \nu(t) \preceq \frac{d}{2}\mathbb{1} \right\}.$$

Each $\hat{V}_t(\nu(t))$ contains an open subset, which contains the actual initial state in its interior. That is, the intersection of $\hat{V}_t(\nu(t))$ is not empty. Furthermore, the intersection of a finite number of open subsets is an open subset. Therefore, any $V_T(\nu_T)$ contains an open subset. ■

Remark 3.2: Theorem 3.1 can be extended to nonlinear systems under a suitable stability assumption. For nonlinear systems, $V_T(\nu_T)$ is defined by a set of nonlinear algebraic equations. ◁

Theorem 3.1 implies that the set of initial states estimated from the quantized output is characterized by a finite set of linear inequalities for Schur stable systems. If a system is unstable, this is not true, which can be exemplified by the following scalar system:

$$\begin{cases} x(t+1) = ax(t),\ x(0) = x_0, \\ \nu(t) = \mathcal{Q}(cx(t)). \end{cases}$$

The output can be described by

$$\nu(t) = \mathcal{Q}(ca^t x_0),$$

i.e.

$$\frac{\nu(t)}{ca^t} - \frac{d}{2ca^t} < x_0 \leq \frac{\nu(t)}{ca^t} + \frac{d}{2ca^t}.$$

For the sake of simplicity, let $a > 1$ and $c > 0$. Then, ca^t can be arbitrary large as time evolves, and thus the above range can be made arbitrary small.

The above discussion for unstable systems implies that if the absolute values of a and c are large, then the initial state is less private for the same time interval. This leads to the natural observation even for a stable system: if the absolute values of elements of $\mathcal{O}_T$ are large, i.e., the system is highly observable, then the initial state is less private.

B. Taking Interconnections into Consideration

In this subsection, we consider the problem setting in Scenario 2.1. To consider external input to the subsystem (1), we define the following matrix and vector:

$$H_0 := 0,$$
$$H_T := \begin{bmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ CB & 0 & \cdots & \cdots & 0 \\ CAB & \ddots & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ CA^{T-1}B & \cdots & CAB & CB & 0 \end{bmatrix},$$
$$u_T = \begin{bmatrix} u^\top(0) & u^\top(1) & \cdots & u^\top(T-1) \end{bmatrix}.$$

For the input sequence u_T and output sequence ν_T of the subsystem (1), the initial state x_0 belongs to the following set:

$$W_T(\nu_T, u_T) := \left\{ x_0 \in \mathbb{R}^{n_1} : -\frac{d}{2}\mathbb{1} \prec \mathcal{O}_T x_0 + H_T u_T - \nu_T \preceq \frac{d}{2}\mathbb{1} \right\}. \tag{8}$$

Note that under Scenario 2.1, $u(t)$ and $\nu(t)$ are bounded. In fact, the interconnected system can be described as

$$\begin{bmatrix} x(t+1) \\ \xi(t+1) \end{bmatrix} = \begin{bmatrix} A & BH \\ GC & F \end{bmatrix} \begin{bmatrix} x(t) \\ \xi(t) \end{bmatrix} + \begin{bmatrix} B & 0 \\ 0 & G \end{bmatrix} \begin{bmatrix} \mathcal{Q}(\eta(t)) - \eta(t) \\ \mathcal{Q}(y(t)) - y(t) \end{bmatrix}. \tag{9}$$

The Schur stability of the system matrix and

$$-\frac{d}{2}\mathbb{1} \prec \begin{bmatrix} \mathcal{Q}(\eta(t)) - \eta(t) \\ \mathcal{Q}(y(t)) - y(t) \end{bmatrix} \preceq \frac{d}{2}\mathbb{1}$$

imply the boundedness of $(x(t), \xi(t))$ and consequently of $(u(t), \nu(t)) = (\mathcal{Q}(G\xi(t)), \mathcal{Q}(Cx(t)))$.

As described above, the effect of quantization can be modeled as bounded disturbance. Because of this, typically three types of trajectories are observed for the system (9) as shown in the following example.

Example 3.3: Suppose that the subsystems (1) and (2) are identical and given by

$$A = F = \begin{bmatrix} 1 & 0.01 \\ -0.01 & 0.99 \end{bmatrix}, \; B = G = \begin{bmatrix} 0 \\ 0.01 \end{bmatrix}$$
$$C = H = \begin{bmatrix} 0.7 & -0.8 \end{bmatrix}.$$

Each subsystem and the interconnected system with $u = \eta$ and $\nu = y$ are Schur stable. Let the quantization step be $d = 1$. In this case, as in Fig.1, the trajectories of y and η converge to the origin. Next, we consider different output matrices

$$C = H = \begin{bmatrix} 0.8 & 0.8 \end{bmatrix}. \tag{10}$$

In this case, as shown in Fig.2, there are off-sets for trajectories due to the effect of quantization. Finally, we choose

$$C = H = \begin{bmatrix} 0.8 & -0.8 \end{bmatrix}. \tag{11}$$

Then, each output trajectory is periodic as confirmed in Fig.3. ◁

In the above three cases, we have similar observation for $W_T(\nu_T, u_T)$ as in Theorem 3.1 without the proof.

Corollary 3.4: Under Scenario 2.1, suppose that y and η converge to certain values or periodic orbits. Then, for any $x_0 \in \mathbb{R}^{n_1}$, there exists $T = T(x_0) \in \mathbb{Z}_+$ such that $W_T(\nu_T, u_T) = W_{T+i}(\nu_{T+i}, u_{T+i})$, $i \in \mathbb{Z}_+$. ◁

Corollary 3.4 implies that owing to quantization, the initial state of the subsystem (1) is not uniquely determined even

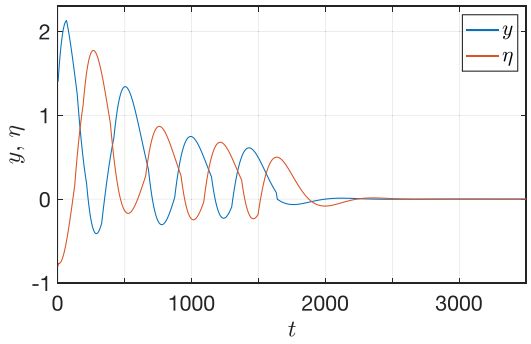

Fig. 1. Trajectories of y and η of the interconnected system when $C = H = [0.7 \; -0.8]$

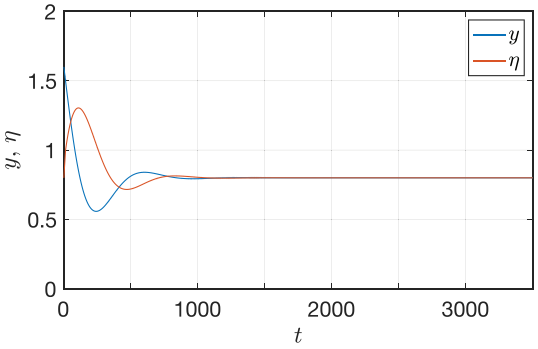

Fig. 2. Trajectories of y and η of the interconnected system when $C = H = [0.8 \; 0.8]$

if the subsystem is observable. However, as illustrated by Example 3.3, quantization degenerates control performances. Therefore, there is a trade-off between privacy and control performances as typically observed in various privacy problems, see e.g. [1]–[4].

C. Observer Design

In the previous subsections, we have shown that the set where the initial state belongs is described by a finite set of linear inequalities for Schur stable systems. Then, the initial state is not uniquely determined by the quantized output. For estimating the system state instead of the initial state, one may design an observer. In this subsection, we consider observer design without assuming stability.

Consider the standard Luenberger observer for the system (1) with the quantized output:

$$z(t+1) = Az(t) + Bu(t) + L(Cz(t) - \mathcal{Q}(y(t))). \quad (12)$$

Then, the error $e := z - x$ satisfies

$$e(t+1) = (A+LC)e(t) + L(y(t) - \mathcal{Q}(y(t))). \quad (13)$$

Due to the quantization error $y(t) - \mathcal{Q}(y(t))$, the estimation error $e(t)$ does not converge to zero in general. It is desirable to design an observer such that e is less sensitive with respect to $y(t) - \mathcal{Q}(y(t))$. Such an observer design reduces to a linear matrix inequality (LMI). Since the proof is a simple application of the bounded real lemma [15], this is omitted.

Proposition 3.5: The H_∞-norm of the error dynamics (13) from the quantization error $y(t) - \mathcal{Q}(y(t))$ to the state estimation error $e(t)$ is not greater than $\gamma > 0$ if and only if the following LMI has solutions P and Y.

$$\begin{bmatrix} P & 0 & (PA+YC)^T & I \\ 0 & \gamma^2 I & Y^T & 0 \\ PA+YC & Y & P & 0 \\ I & 0 & 0 & I \end{bmatrix} > 0.$$

Moreover, for $L := P^{-1}Y$, the H_∞-norm is not greater than γ. ◁

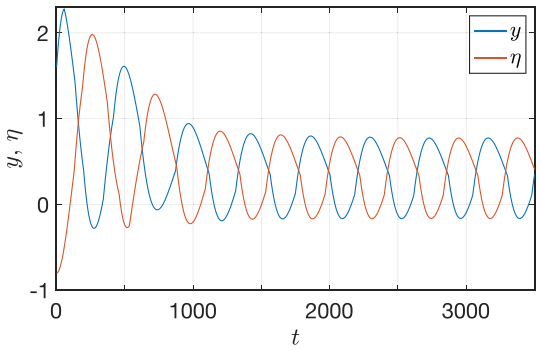

Fig. 3. Trajectories of y and η of the interconnected system when $C = H = [0.8 \ -0.8]$

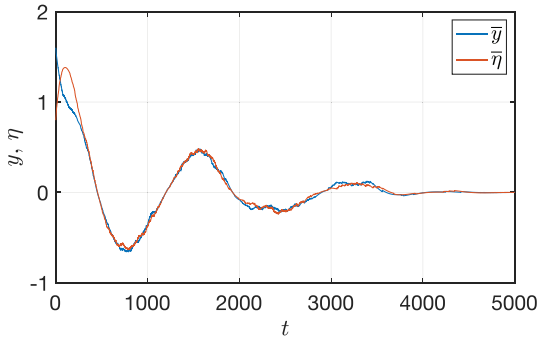

Fig. 4. Trajectories of $\bar{y}$ and $\bar{\eta}$ of the interconnected system when $C = H = [0.8 \ 0.8]$ with uniform noise

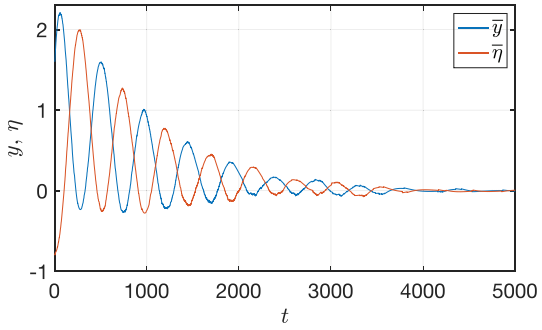

Fig. 5. Trajectories of $\bar{y}$ and $\bar{\eta}$ of the interconnected system when $C = H = [0.8 \ -0.8]$ with uniform noise

IV. Initial State Privacy under Dithered Quantization

A. Improvement of Both Control and Privacy Performances

In the literature, it is observed that effects of quantization errors can be made smaller by adding noise because noise can eliminate periodic behavior caused by quantization. Such a technique is called dithering [10], [11]. In this section, we confirm that dithering improves not only control performance but also privacy performance. In other words, dithering can be a tool to improve the overall trade-off between these performances under quantization.

Now, we consider the following interconnections:

$$\begin{aligned} \bar{\nu} &= \mathcal{Q}(y + w_y), \\ \bar{u} &= \mathcal{Q}(\eta + w_\eta), \end{aligned} \quad (14)$$

where $w_y, w_\eta : \mathbb{Z} \to [-d/2, d/2]$ are uniform distributed random noise. We confirm the utility of dithering thorough an example.

Example 4.1 (Continuation of Example 3.3): Fig.4 and Fig.5 show the trajectories of y and η with dithered quantization (14) when the output matrices are (10) and (11), respectively. In both cases, outputs are sufficiently close to the origin. ◁

As shown in Example 4.1, adding noise can increase control performance in the sense of the convergence to the origin. From the viewpoint of privacy, it is easy to see that dithering increases privacy performance, where noise is not added formally, or said differently, some noise that is equal to zero with probability one is added.

Proposition 4.2: Consider the same assumptions as in Corollary 3.4, and $\bar{u}_T$ and $\bar{\nu}_T$ denote the input and output sequences of the subsystem (1) when the interconnection is (14). Then, we have the following

$$\begin{aligned}&\mathbb{P}(x_0 \in W_T(\omega_T, v_T)|(\omega_T, v_T) = (\bar{\nu}_T, \bar{u}_T))\\ &< \mathbb{P}(x_0 \in W_T(\omega_T, v_T)|(\omega_T, v_T) = (\nu_T, u_T)),\end{aligned}$$

Proof: It is clear that $\mathbb{P}(x_0 \in W_T(\omega_T, v_T)|(\omega_T, v_T) = (\nu_T, u_T)) = 1$ when noise is not added, and $\mathbb{P}(x_0 \in W_T(\omega_T, v_T)|(\omega_T, v_T) = (\bar{\nu}_T, \bar{u}_T)) < 1$ when noise is added. ∎

Proposition 4.2 is intuitive and follows from the fact that

$$|y - \mathcal{Q}(y)| \leq |y - \mathcal{Q}(y + w_y)|. \tag{15}$$

However, it is difficult to compute the probability $\mathbb{P}(x_0 \in W_T(\omega_T, v_T)|(\omega_T, v_T) = (\bar{\nu}_T, \bar{u}_T))$. To evaluate the effect of dithering, it can still be helpful to compute the probability when $T = 0$, i.e. to check how difficult it is to estimate y from $\mathcal{Q}(y + w_y)$. To have a close look of the effect of the uniform noise, we change the range of w_y.

Proposition 4.3: For the uniform distributed random variable $w : \mathbb{Z} \to [-a/2, a/2]$, $0 < a \leq d$, it follows that

$$\mathbb{P}\left(z \in \left(nd - \frac{d}{2}, nd + \frac{d}{2}\right] \middle| \mathcal{Q}(z + w) = nd\right) = \frac{2d - a}{2d}.$$

Proof: The proof is given in Appendix. ∎

B. Observer Design

In this subsection, we revisit the observer (12) and investigate the estimation error. The following theorem shows that the error can be made small if one designs the observer having a small H_∞-norm using Proposition 3.5.

Theorem 4.4: Consider the observer (12) for the system (1) with the quantized output. Suppose that $A + LC$ is Schur stable, and the H_∞-norm of the observer (12) from the quantization error $y(t) - \mathcal{Q}(y(t))$ to the state estimation error $e(t)$ is not greater than $\gamma > 0$. Then, it follows that

$$\lim_{t\to\infty} \mathbb{E}[|e(t)|^2] \leq \frac{d^2\gamma^2}{2}. \tag{16}$$

Proof: From (12), $e(t)$ can be described by

$$e(t) = (A + LC)^t e(0) + \sum_{k=0}^{t} h_k(y(t-k) - \mathcal{Q}(y(t-k))),$$

where

$$h_k := \begin{cases} 0, & k = 0,\\ (A + LC)^{k-1}L, & k > 0.\end{cases}$$

Since $\lim_{t\to\infty}(A + LC)^t = 0$, one takes $e(0) = 0$ without loss of generality.

Note that $y(t) - \mathcal{Q}(y(t))$ is uncorrelated with respect to time [12]. Therefore, we have

$$\mathbb{E}[|e(t)|^2] = \sum_{k=0}^{t} |h_k|^2 \mathbb{E}[|y(t-k) - \mathcal{Q}(y(t-k))|^2]$$

According to [12], it follows that

$$\mathbb{E}[|y(t-k) - \mathcal{Q}(y(t-k))|^2] \leq \frac{d^2}{4}.$$

From the definition of the H_∞-norm, $\sum_{k=0}^{t} |h_k|^2 \leq \gamma^2$. From these two, $\mathbb{E}[|e(t)|^2]$ is bounded as

$$\mathbb{E}[|e(t)|^2] \leq \frac{d^2\gamma^2}{2},\ \forall t \in \mathbb{Z}_+.$$

From its definition, $\mathbb{E}[|e(t)|^2]$ is an increasing sequence of t. Therefore, $\mathbb{E}[|e(t)|^2]$ converges to some value, and consequently (16) holds. ∎

When there is measurement noise, the Kalman filter is employed in most of the cases. However, in this problem setting, due to the property (16), random variables $h_k(y(t) - \mathcal{Q}(y(t)))$ do not satisfy the Lindeberg condition [14]. That is, it is not clear if $\sum_{k=0}^{t} h_k(y(t-k) - \mathcal{Q}(y(t-k)))$ tends to a normal distribution, and there is no theoretical guarantee that the Kalman filter works for this problem. This is another advantage of dithering from the privacy viewpoint.

Using Example 4.1, we confirm that dithering improves control performance. One may expect similar improvement for observer design. However, there is an essential difference between the feedback interconnection and observer. In the feedback interconnection, $y - \mathcal{Q}(y)$ depends on the state ξ of the other subsystem. This dependence is a key property for improvement of control performance by dithering [13]. In observer design, the quantization error $y - \mathcal{Q}(y)$ does not depend on the observer state z in contrast to the feedback interconnection. Therefore, a similar improvement may not exist for the observer.

V. Conclusion

In this paper, we have proceeded with privacy analysis under quantization and dithering, respectively. It is known that quantization degenerates control performance, and dither attenuates the degeneration. In contrast, both quantizer and dither have potential to improve privacy performance as discussed in this paper. Therefore, dithering can be a useful tool to improve the trade-off between control and private performances under quantization. In the future, we plan to look into different types of quantizers and to examine other control performance indices.

Appendix

Proof: [Proposition 4.3] Without loss of generality, let $n = 0$. From Bayes' theorem, it follows that

$$\begin{aligned}&\mathbb{P}\left(z \in \left(-\frac{d}{2}, \frac{d}{2}\right] \middle| \mathcal{Q}(z + w) = 0\right)\\ &= \frac{\mathbb{P}\left(z \in \left(-\frac{d}{2}, \frac{d}{2}\right]\right)}{\mathbb{P}(\mathcal{Q}(z + w) = 0)} \mathbb{P}\left(\mathcal{Q}(z + w) = 0 \middle| z \in \left(-\frac{d}{2}, \frac{d}{2}\right]\right).\end{aligned} \tag{17}$$

When $n = 0$, z belongs to $(-(a + d)/2, (a + d)/2]$, which implies

$$\mathbb{P}\left(z \in \left(-\frac{d}{2}, \frac{d}{2}\right]\right) = \frac{d}{a + d}.$$

Next, we compute $\mathbb{P}(\mathcal{Q}(z+w)=0|z\in(-d/2,d/2])$. It follows that

$$\begin{aligned}
&\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)\\
&=\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z<-\frac{d-a}{2}\right)\\
&\quad\times\mathbb{P}\left(z<-\frac{d-a}{2}\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)\\
&\quad+\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|-\frac{d-a}{2}\le z\le\frac{d-a}{2}\right)\\
&\quad\times\mathbb{P}\left(-\frac{d-a}{2}\le z\le\frac{d-a}{2}\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)\\
&\quad+\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|\frac{d-a}{2}<z\right)\\
&\quad\times\mathbb{P}\left(\frac{d-a}{2}<z\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right).
\end{aligned}$$

We compute each probability as follows:

$$\begin{aligned}
&\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z<-\frac{d-a}{2}\right)=\frac{d+a+2z}{2(a+d)},\\
&\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|-\frac{d-a}{2}\le z\le\frac{d-a}{2}\right)=1,\\
&\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|\frac{d-a}{2}<z\right)=\frac{d+a-2z}{2(a+d)},
\end{aligned}$$

and

$$\begin{aligned}
&\mathbb{P}\left(z<-\frac{d-a}{2}\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)=\frac{a}{2d},\\
&\mathbb{P}\left(-\frac{d-a}{2}\le z\le\frac{d-a}{2}\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)=\frac{d-a}{d},\\
&\mathbb{P}\left(\frac{d-a}{2}<z\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)=\frac{a}{2d}.
\end{aligned}$$

Combining them yields

$$\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)=\frac{2d-a}{2d}.$$

Finally, we compute $\mathbb{P}(\mathcal{Q}(z+w)=0)$. It follows that

$$\begin{aligned}
&\mathbb{P}(\mathcal{Q}(z+w)=0)\\
&=\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z\in\left(-\frac{a+d}{2},-\frac{d}{2}\right]\right)\\
&\quad\times\mathbb{P}\left(z\in\left(-\frac{a+d}{2},-\frac{d}{2}\right]\right)\\
&\quad+\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)\\
&\quad\times\mathbb{P}\left(z\in\left(-\frac{d}{2},\frac{d}{2}\right]\right)\\
&\quad+\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z\in\left(\frac{d}{2},\frac{a+d}{2}\right]\right)\\
&\quad\times\mathbb{P}\left(z\in\left(\frac{d}{2},\frac{a+d}{2}\right]\right)
\end{aligned}$$

Again, we compute each probability as follows:

$$\begin{aligned}
&\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z\in\left(-\frac{a+d}{2},-\frac{d}{2}\right]\right)=\frac{d+a+2z}{2(a+d)},\\
&\mathbb{P}\left(\mathcal{Q}(z+w)=0\middle|z\in\left(\frac{d}{2},\frac{a+d}{2}\right]\right)=\frac{d+a-2z}{2(a+d)},
\end{aligned}$$

and

$$\begin{aligned}
&\mathbb{P}\left(z\in\left(-\frac{a+d}{2},-\frac{d}{2}\right]\right)=\frac{a}{2(a+d)},\\
&\mathbb{P}\left(z\in\left(\frac{d}{2},\frac{a+d}{2}\right]\right)=\frac{a}{2(a+d)}.
\end{aligned}$$

Therefore, we obtain

$$\mathbb{P}(\mathcal{Q}(z+w)=0)=\frac{d}{a+d}.$$

In summary, substituting all computed results into (17) yields

$$\mathbb{P}\left(z\in\left(-\frac{d}{2},\frac{d}{2}\right]\middle|\mathcal{Q}(z+w)=0\right)=\frac{2d-a}{2d}$$

That completes the proof. ■

REFERENCES

[1] F. Farokhi and H. Sandberg, "Ensuring privacy with constrained additive noise by minimizing Fisher information," *Automatica*, vol. 99, pp. 275–288, 2019.

[2] J. Cortés, G. E. Dullerud, S. Han, J. L. Ny, S. Mitra, and G. Pappas, "Differential privacy in control and network systems," *Proc. 55th IEEEConference on Decision and Control*, pp. 4252–4272, 2016.

[3] Y. Kawano and M. Cao, "Design of privacy-preserving dynamic controllers," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3863–3878, 2020.

[4] Y. Kawano, K. Kashima, and M. Cao, "Modular control under privacy protection: fundamental trade-offs," *Automatica*, vol. 127, p. 109518, 2021.

[5] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," *Proc. 54th IEEE Conference on Decision and Control*, pp. 6836–6843, 2015.

[6] F. Farokhi, I. Shames, and N. Batterham, "Secure and private control using semi-homomorphic encryption," *Control Engineering Practice*, vol. 67, pp. 13–20, 2017.

[7] C. Murguia, I. Shames, F. Farokhi, and D. Nešić, "On privacy of quantized sensor measurements through additive noise," *Proc. 2018 IEEE Conference on Decision and Control*, pp. 2531–2536, 2018.

[8] F. Farokhi, "Development and analysis of deterministic privacy-preserving policies using non-stochastic information theory," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2567–2576, 2019.

[9] L. Wang, I. R. Manchester, J. Trumpf, and G. Shi, "Initial-value privacy of linear dynamical systems," *Proc. 59th IEEE Conference on Decision and Control*, pp. 3108–3113, 2020.

[10] R. A. Ulichney, "Dithering with blue noise," *Proceedings of the IEEE*, vol. 76, no. 1, pp. 56–79, 1988.

[11] S. P. Lipshitz, R. A. Wannamaker, and J. Vanderkooy, "Quantization and dither: A theoretical survey," *Journal of the audio engineering society*, vol. 40, no. 5, pp. 355–375, 1992.

[12] R. Morita, S.-i. Azuma, and T. Sugie, "Performance analysis of random dither quantizers in feedback control systems," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 11 296–11 301, 2011.

[13] K. Kashima and D. Inoue, "Stationary performance evaluation of control systems with random dither quantization," *Proc. 2014 European Control Conference*, pp. 1625–1630, 2014.

[14] P. Billingsley, *Probability and Measure*. John Wiley & Sons, 2008.

[15] R. E. Skelton, T. Iwasaki, and D. E. Grigoriadis, *A Unified Algebraic Approach to Control Design*. CRC Press, 1997.